Manuel
Villoldo
Martinez

Firmado digitalmente por Manuel Villoldo Martinez
Nombre de reconocimiento (DN): c=ES, cn=Manuel Villoldo Martinez, email=mvilloldo@camaravalencia.com, serialNumber=74503625R, sn=Villoldo Martinez, givenName=Manuel, 1.3.6.1.4.1.17326.30.3=Q4673002D, o=CÁMARA DE COMERCIO DE VALENCIA, ou=MANTENIMIENTO CONSERJERIA, title=MANTENIMIENTO CONSERJERIA, 2.5.4.13=Qualified Certificate: CAM-PF-SW-KPSC
Fecha: 2015.11.13 08:43:25 +01'00'

Publicación Certificada

Manual de usuario

Sumario

Revisiones 3
Glosario 4
Introducción 8
A quién va dirigido este documento 8
Antes de comenzar 9
Modos de uso 10
Portal web 10
Acceso usuarios 10
Cabecera 11
Inicio 11
Nueva publicación 12
Eliminar publicación 15
Consultar crédito 16
Cambiar contraseña 17
Posibles respuestas 18
Cerrar sesión 18
Estados de las publicaciones 19

Revisiones

Revisión	Fecha	Cambios	Autor
1.0	20/12/2010	Primera redacción	EGG
1.1	03/01/2011	Revisión y aprobación	RLG
1.2	05/02/2011	Actualización WebServices	EGO

Glosario

Algoritmo: Secuencia de reglas e instrucciones que indican el procedimiento a partir del cual se resuelve un problema. La firma digital de un documento es el resultado de aplicar cierto algoritmo matemático, denominado función hash, a su contenido, y seguidamente aplicar el algoritmo de firma (en el que se emplea una clave privada) al resultado de la operación anterior, generando la firma electrónica o digital.

Autenticación: La autenticación es la situación en la cual se puede verificar que un documento ha sido elaborado (o pertenece) a quien el documento dice. Aplicado a la verificación de la identidad de un usuario, la autenticación se produce cuando el usuario puede aportar algún modo de que se pueda verificar que dicha persona es quien dice ser, a partir de ese momento se considera un usuario autorizado. Otra manera de definirlo seria, la capacidad de determinar si una determinada lista de personas ha establecido su reconocimiento sobre el contenido de un mensaje.

Autoridad de Certificación: Es la entidad de confianza, responsable de emitir y revocar los certificados electrónicos, utilizados en la firma electrónica. La Autoridad de Certificación, por sí misma o mediante la intervención de una Autoridad de Registro, verifica la identidad del solicitante de un certificado antes de su expedición o, en caso de certificados expedidos con la condición de revocados, elimina la revocación de los certificados al comprobar dicha identidad.

Autoridad de sellado del tiempo: Actúa como tercera parte de confianza testificando la existencia de dichos datos electrónicos en una fecha y hora concretos.

Caducidad del certificado digital: El certificado digital tiene un período de vigencia que consta en el mismo certificado. Generalmente es de 2 años, aunque por ley se permite una vigencia de hasta 5 años. Una vez el certificado haya caducado, no se podrán utilizar los servicios ofrecidos por la Administración que requieran firma electrónica, y cualquier firma electrónica que se haga a partir de ese momento no tendrá validez.

Certificado digital: Documento en soporte informático emitido y firmado por la Autoridad de Certificación, que garantiza la identidad de su propietario.

Certificado reconocido: Certificado expedido por un Prestador de Servicios de Certificación que cumple los requisitos establecidos en la Ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten, de conformidad con lo que dispone el capítulo II del Título II de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica.

Confidencialidad: Se trata de la cualidad que debe poseer un documento o archivo para que este solo se entienda de manera comprensible o sea leído por la persona o sistema que este autorizado. De esta manera se dice que un documento (o archivo o mensaje) es confidencial si y solo si puede ser comprendido por la persona o entidad a quien va dirigida o esté autorizada. En el caso de un mensaje esto evita que exista una intercepción de este y que pueda ser leído por una persona no autorizada.

Contrafirma: Firma electrónica realizada sobre una firma anterior, y no sobre todo el documento anterior.

CRL: Lista de Certificados Revocados de las autoridades de certificación, donde figuran exclusivamente la relación de certificados revocados o suspendidos.

Dispositivo seguro de creación de Firma: instrumento que sirve para aplicar los datos de creación de firma cumpliendo con los requisitos que establece el artículo 24.3 de la Ley 59/2003, de 19 de diciembre, de Firma Electrónica. Certificación common criteria certification EAL4+ based on CWA 14169.

ETSI: European Telecommunications Standards Institute (ETSI) o Instituto Europeo de Normas de Telecomunicaciones, es una organización de estandarización de la industria de las telecomunicaciones (fabricantes de equipos y operadores de redes) de Europa, con proyección mundial. Principal abanderado del estándar XMLDSig o XAdES como formato estandarizado para la firma electrónica avanzada.

Firma electrónica: Conjunto de datos, en forma electrónica, anejos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge. Existen 3 tipos de firma electrónica: firma electrónica simple, avanzada y reconocida.

Firma electrónica simple: Conjunto de datos, en forma electrónica, anejos a otros datos.

Firma electrónica avanzada: Firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.

Firma electrónica reconocida: Se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma. La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.

Función hash: es una operación que se realiza sobre un conjunto de datos de cualquier tamaño, de forma que el resultado obtenido es otro conjunto de datos de tamaño fijo, independientemente del

tamaño original, y que tiene la propiedad de estar asociado unívocamente a los datos iniciales, es decir, es imposible encontrar dos mensajes distintos que generen el mismo resultado al aplicar la Función hash.

Hash o Huella digital: resultado de tamaño fijo que se obtiene tras aplicar una función hash a un mensaje y que cumple la propiedad de estar asociado unívocamente a los datos iniciales.

Integridad: La integridad es la cualidad que posee un documento o archivo que no ha sido alterado y que además permite comprobar que no se ha producido manipulación alguna en el documento original.

Listas de Revocación de Certificados o Listas de Certificados Revocados: lista donde figuran exclusivamente las relaciones de certificados revocados o suspendidos (no los caducados).

No repudio: El emisor que firme electrónicamente un documento no podrá negar que envió el mensaje original, ya que éste es imputable al emisor por medio de la clave privada que únicamente conoce él y que está obligado a custodiar. El no repudio permite, además, comprobar quién participó en una transacción.

El no repudio o irrenunciabilidad es un servicio de seguridad estrechamente relacionado con la autenticación y que permite probar la participación de las partes en una comunicación. La diferencia esencial con la autenticación es que la primera se produce entre las partes que establecen la comunicación y el servicio de no repudio se produce frente a un tercero

Prestador de Servicios de Certificación o PSC: Persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica. Ver Autoridad de Certificación.

PIN: Secuencia de caracteres que permiten el acceso a los certificados. Clave Personal de Acceso.

Renovación: La renovación consiste en solicitar un nuevo certificado mediante un certificado vigente pero que está a punto de caducar. De esta manera, antes de la caducidad de un certificado se puede solicitar la renovación y esto implica que se emita un nuevo certificado válido.

Revocación: Anulación definitiva de un certificado digital a petición del suscriptor, o por propia iniciativa de la autoridad de certificación en caso de duda de la seguridad de las claves. La revocación es un estado irreversible. Se puede solicitar la revocación de un certificado después de una situación de suspensión o por voluntad de las personas autorizadas a solicitarla. De la misma manera, en el caso de un certificado suspendido, si ha pasado el periodo de suspensión máximo, si el certificado no ha sido habilitado, pasa a estar definitivamente revocado. Cuando la entidad de certificación revoca o suspende un certificado, ha de hacerlo constar en las Listas de Certificados Revocados (CRL), para hacer público este hecho. Estas listas son públicas y deben estar siempre disponibles.

Sello de tiempo: Mecanismo que permite demostrar que una serie de datos han existido y no han sido alterados desde un instante específico en el tiempo. Este protocolo se describe en el RFC 3161 de la ETSI y está en el registro de estándares de Internet.

Una Autoridad de Sellado de Tiempo actúa como tercera parte de confianza testificando la existencia de dichos datos electrónicos en una fecha y hora concretos. Las normas europeas TS 101 733 y TS 101 903 establecen dos modalidades de firma que incluyen sellado de tiempo. La variante ES-T añade el sellado a una firma básica (BES) y la variante ES-C añade, además del sellado de tiempo, información sobre la ruta en la que se puede verificar la validez del certificado obtenido de una consulta OCSP o de CRL. Además estas normas prevén la modalidad ES-XL que incluye información sobre el estado de revocación del certificado. De esta forma se obtiene una firma completa que libera al receptor de la firma del problema de deducir de la firma o del certificado la forma de comprobar la validez del certificado que puede variar de PSC en PSC.

Tarjeta inteligente (smartcard): Cualquier tarjeta con circuitos integrados que permiten la ejecución de cierta lógica programada.

TSA: Contracción del vocablo inglés “Time-Stamping Authority”. Correspondiente al término Autoridad de Sellado de Tiempo.

TSU: Contracción del vocablo inglés “time-stamp unit”. Corresponde a una Unidad específica de sellado de tiempo, perteneciente a los TSS de la TSA. Es la unidad desde la que se crean y firman en nombre de la TSA los sellos digitales de tiempo.

Validar documento: Mecanismo que permite verificar si un documento o fichero ha sido alterado, además de identificar con seguridad a la persona que lo ha firmado, y opcionalmente, garantizar el momento exacto (fecha y hora) en que se produjo la firma.

Introducción

Según el artículo 42 de la Ley 30/2007 de 30 de Octubre "el sistema informático que soporte el perfil de contratante deberá contar con un dispositivo que permita acreditar fehacientemente el momento de inicio de la difusión pública de la información que se incluya en el mismo". De obligado cumplimiento para instituciones públicas, es muy recomendable la adaptación a sus requisitos de las corporaciones privadas, pues proporciona un mecanismo de mayor seguridad y control frente a posibles litigios, y de cara a ofrecer al cliente un servicio de mayor calidad, reforzando la imagen de vanguardia tecnológica.

Publicación Certificada de Camerfirma, mediante la firma de la publicación realizada en un "dispositivo seguro de creación de firma", y el sello de tiempo de una Autoridad de Certificación reconocida, acredita fehacientemente el inicio de la difusión de la publicación.

La solución de Publicación Certificada de Camerfirma ofrece un servicio de certificación de publicaciones sencillo y eficaz. Publicación Certificada de Camerfirma permite certificar la fecha y hora precisas de cualquier tipo de publicación online.

A quién va dirigido este documento

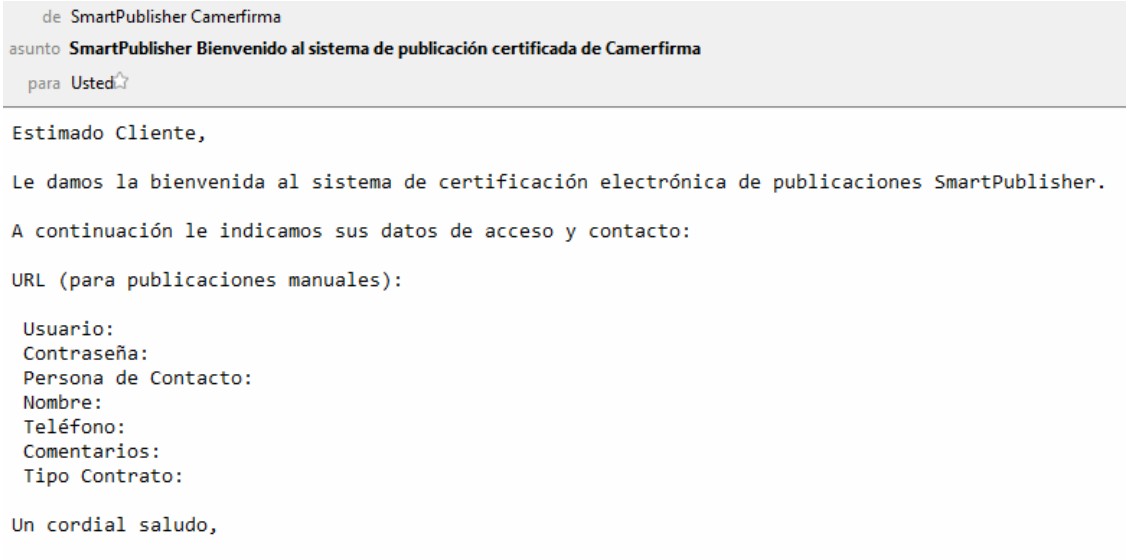
- ***Usuarios finales***, que desean certificar la publicación online de documentos firmados mediante un sistema con plena validez y respaldo legal.

Antes de comenzar

Para empezar a utilizar el servicio de Publicación Certificada es necesario ponerse en contacto con el personal de Camerfirma para que realice el alta en el sistema.

Cuando el alta se haya llevado a cabo correctamente, el sistema nos proveerá vía email de los datos de cuenta y acceso.

El email recibido será similar al siguiente:



de SmartPublisher Camerfirma
asunto **SmartPublisher Bienvenido al sistema de publicación certificada de Camerfirma**
para Usted

Estimado Cliente,

Le damos la bienvenida al sistema de certificación electrónica de publicaciones SmartPublisher.

A continuación le indicamos sus datos de acceso y contacto:

URL (para publicaciones manuales):

Usuario:
Contraseña:
Persona de Contacto:
Nombre:
Teléfono:
Comentarios:
Tipo Contrato:

Un cordial saludo,

Modos de uso

El sistema se integra con los flujos de trabajo existentes del usuario a través de un portal web extremadamente sencillo, o mediante WebServices. Este documento solo hace referencia al portal web para usuarios.

Portal web

Acceso usuarios

Para comenzar a utilizar el sistema accederemos a la dirección web suministrada en el email de alta. Con los datos facilitados en dicho email podremos acceder a la pantalla principal introduciendo el nombre de usuario y la contraseña.

Formalizaremos el acceso pulsando en el botón Entrar.

Posibles respuestas

Mensaje error:

- Por favor introduzca el nombre de usuario: En la casilla Usuario no se ha introducido ningún valor.
- Por favor introduzca la contraseña: En la casilla Contraseña no se ha introducido ningún valor.
- Nombre de usuario o contraseña inválida: Revise sus datos de acceso (Usuario y Contraseña) ya que alguno de estos es incorrecto. Si persiste el error contacte con el administrador del sistema.

Cabecera

Links para navegar por las diferentes pantallas:

- Inicio.
- Nueva Publicación.
- Eliminar Publicación.
- Consultar Crédito.
- Cambiar Contraseña.
- Cerrar Sesión.

Inicio

En inicio (pantalla principal) podremos ver las publicaciones certificadas que hemos efectuado.

Las opciones disponibles son:

- Filtro: búsqueda para acceder a las publicaciones rápidamente
  - Por Fecha de publicación DE: A:
  - Por Título
  - Ordenar por diferentes campos
- Resultado: Muestra los resultados de la búsqueda, por defecto todas
  - Lista con las publicaciones, sus detalles y estado

- Link para visualizar la publicación certificada

- Pie de la página:
  - Campo ordenar
  - Avanzar y retroceder por las diferentes paginas con publicaciones

Publicación Certificada
SmartPublisher
Inicio | Nueva Publicación | Eliminar Publicación | Consultar Crédito | Cambiar Contraseña | Cerrar Sesión
Consulta Publicaciones
Filtro
Fecha de publicación: A:
Título:
Buscar
Resultado
Ente publicador | Título | Expediente | Descripción | Estado | Fecha publicacion | Fecha fin periódica
Consorcio del Mar | Publicación Certificada 2 | EFE6 | Estado actual de las naves marítimas | Firmando | 26/11/2010 17:15:17 | 27/11/2010
Consorcio del Mar | Publicación Certificada 1 | EFE5 | Publicación sobre las condiciones actuales del Mar | Publicada | 26/11/2010 17:12:46 | 00/00/0000
Mostrando registros de 1 a 2
Ordenar por: Fecha publicacion
Ente publicador
Titulo
Expediente
Estado
Fecha publicacion
Ordenar
© 2009 Camerfirma S.A. Todos los derechos reservados.
Powered by Bit4id

Nueva publicación

En esta pantalla podremos iniciar el proceso de certificación de una nueva publicación.

Tendremos que completar obligatoriamente la siguiente información:

- Título: Introduciremos el título de nuestra publicación a certificar
- Original: Introduciremos la URL donde se encuentra nuestro documento a certificar, en formato PDF
- Descripción: Este campo es opcional y nos permite añadir una pequeña descripción o comentarios

- Expediente: Introduciremos el número de expediente del documento a certificar
- Validación periódica: Marcaremos este campo en caso de querer diariamente comprobar la validación y no modificación de nuestro documento
- Fecha Fin: En caso de marcar como validación periódica deberemos introducir la fecha en que finalizará

Una vez completado pulsaremos en Publicar y seremos redirigidos a la página principal donde podremos ver el estado de nuestra publicación.

Posibles respuestas

Mensaje éxito: Publicación en proceso...

Mensaje error:

- La URL del documento original debe contener entre 5 y 300 caracteres: En la casilla URL ha introducido una dirección web no válida.
- El título debe contener entre 5 y 200 caracteres: En la casilla título ha introducido un título no válido.
- La descripción debe contener entre 5 y 500 caracteres En la casilla descripción ha introducido una descripción no válida.
- El departamento debe contener entre 5 y 30 caracteres: En la casilla departamento ha introducido un departamento no válido.

- El expediente debe contener entre 2 y 30 caracteres: En la casilla expediente ha introducido un expediente no válido.
- Debe introducir una fecha: Si la publicación necesita validación periódica deberemos indicar la fecha a partir de la cual ya no se necesitará comprobar el documento.

Eliminar publicación

Esta pantalla es similar a la de inicio:

Publicación Certificada
SmartPublisher
Inicio | Nueva Publicación | Eliminar Publicación | Consultar Crédito | Cambiar Contraseña | Cerrar Sesión
Eliminar Publicación
Filtro
Fecha de publicación: A:
Título:
Buscar
Resultado
Ente publicador | Título | Expediente | Descripción | Estado | Fecha publicacion | Fecha fin periódica
Consorcio del Mar | Publicación Certificada 2 | EFE6 | Estado actual de las naves marítimas | Publicada | 26/11/2010 17:15:17 | 27/11/2010
Consorcio del Mar | Publicación Certificada 1 | EFE5 | Publicación sobre las condiciones actuales del Mar | Publicada | 26/11/2010 17:12:46 | 00/00/0000
Mostrando registros de 1 a 2
Ordenar por: Fecha publicacion
Ordenar
© 2009 Camerfirma S.A. Todos los derechos reservados.

Podremos ver las publicaciones certificadas que hemos efectuado.

Las opciones disponibles son:

- Filtro: búsqueda para acceder a las publicaciones rápidamente
    - Por Fecha de publicación DE: A:
    - Por Título

- Ordenar por diferentes campos

- Resultado: Muestra los resultados de la búsqueda, por defecto todas
  - Listado con las publicaciones, sus detalles y estado
  - Seleccionar la publicación a eliminar
- Pie de la página:
  - Campo ordenar.
  - Avanzar y retroceder por las diferentes paginas con publicaciones.

Los pasos a seguir para eliminar una publicación son los siguientes:

1. Este link nos permitirá seleccionar la publicación a eliminar
2. Seremos redirigidos a una nueva página:

3. Deberemos confirmar que la publicación indicada es realmente la que queremos eliminar.

Mensaje éxito: Eliminado el registro correctamente

Consultar crédito

En esta pantalla podremos comprobar en detalle nuestro consumo de créditos agrupado en:

- Publicaciones:
    - Crédito total consumido: Es la suma total de todas las publicaciones efectuadas desde el alta en el servicio.
    - Crédito consumido: Nos indica el crédito consumido desde la última recarga.
    - Crédito restante: Nos indica el crédito restante total.
- Publicaciones periódicas:
    - Crédito periódicas total consumido: Es la suma total de todas las publicaciones periódicas efectuadas desde el alta en el servicio.
    - Crédito periódicas consumido: Nos indica el crédito consumido desde la última recarga.
    - Crédito periódicas restante: Nos indica el crédito restante total.

Publicación Certificada
SmartPublisher
Inicio | Nueva Publicación | Eliminar Publicación | Consultar Crédito | Cambiar Contraseña | Cerrar Sesión
Consulta Crédito
Detalles
Usuario: Mariona
Crédito total consumido: 1 créditos
Crédito consumido*: 1 créditos
Crédito restante: 4 créditos
Crédito periódicas total consumido: 1 créditos
Crédito periódicas consumido*: 1 créditos
Crédito periódicas restante: 4 créditos
Notas: *Crédito consumido desde la última recarga o facturación.

Cambiar contraseña

Para establecer una nueva contraseña de acceso:

1. Introduciremos la contraseña antigua.
2. Introduciremos la nueva contraseña
3. Volveremos a introducir la nueva contraseña.

Posibles respuestas

Mensaje éxito: Actualización satisfactoria

Mensaje error:

- Por favor introduzca la contraseña: En la casilla Contraseña no se ha introducido ningún valor.
- Por favor introduzca su nueva contraseña: En la casilla nueva Contraseña no se ha introducido ningún valor.
- Las nuevas contraseñas no coinciden: Asegúrese de que su nueva contraseña es introducida en las dos casillas correctamente.
- Actualización terminada: No hay ningún cambio a actualizar.

Cerrar sesión

Realiza la salida y desconexión del sistema.

Para una correcta desconexión se aconseja siempre su uso antes de cerrar el navegador.

Estados de las publicaciones

- **Publicada:** El proceso de certificación ha finalizado correctamente, ya puede consultar y ver su publicación. También nos indica que ya está disponible en el portal público.
- **Firmando:** Nos indica que está en proceso de certificación, espere unos instantes para su finalización.
- **Descargando:** Nos indica que está en proceso de descarga del documento para su posterior verificación y firma.
- **URL no válida 2:** Nos indica que el proceso ha finalizado con error ya que no ha podido descargar el documento en la URL Original. Seguramente la dirección es incorrecta, vuelva a intentarlo de nuevo tras comprobarla.
- **Documento sin firmar:** La Firma en el documento a certificar no es correcta, asegúrese de haberlo firmado correctamente.
- En caso de cualquier otro tipo de estado deberá contactar con el administrador del sistema.

Más información:

www.camerfirma.com

soporte@camerfirma.com